OrionX.net

The OrionX Constellation
Blockchain and Cryptocurrencies

Evolution

Third CryptoSuper 500 List: A Hundred ExaHashes

Hashrate for Bitcoin Doubles each Seven Months

Stephen Perrenod
November 2019

Note: This paper is an analysis of the technologies and trends surrounding blockchain and cryptocurrencies. It is not, and must not be considered as, financial, investment, or legal advice.

Bitcoin as global money

"Money has become information. Bitcoin is energy securely encapsulated as information. Electrons to eternal bits. Money in the Internet, and only in the Internet." @moneyordebt

One Bitcoin has the value of 165 barrels of oil. Bitcoin is encapsulated energy, transformed through a cryptographic "mining" process into secure, immutable information. This new form of money can be transferred across the globe at low cost in a matter of minutes.

Actually, it is already "around the globe" since it resides in thousands of "full nodes" as a widely replicated, decentralized ledger. You don't move Bitcoin, you just transfer ownership to a new private key holder.

Around three-quarters of Bitcoin is produced from renewable energy sources. The value of one hundred million barrels of oil is being produced per annum as new Bitcoins.

Review of prior two CryptoSuper lists

Cryptocurrrency mining is a specialized form of supercomputing. It relies on large clusters of mining rigs with substantial power and cooling requirements, and the operators of these seek out low cost power and cooling locations. Hydropower access is especially favored, and it has been estimated that some 75% or so of power used in crypto mining by large compute farms is sourced from renewables.

One difference is that these are mining pools, and they often welcome anyone to contribute their own compute resources from anywhere in the world, and share in the crypto mining rewards. The problem is inherently embarrassingly parallel since one must make billions or trillions of guesses at a 'nonce' before computing the winning result. The pool concept is not totally different from the office pool for lottery tickets. Your chances of winning something are significantly enhanced by joining a pool. Naturally, the reward must then be shared, proportionately with the hash rate contribution.

Because cryptocurrency mining is inherently a decentralized process, there is also an increasing trend toward operators locating major crypto mining resources in several countries, creating global pools. China has tightened up on some operators, rationing their access to electric power, and this has encouraged migration of resources to Europe and North America.

Our first two lists were released in November 2018, and June 2019, in conjunction with the large supercomputer conferences in the US and Germany. Here is a blog on the second list, and here is a slide presentation for the second list.

BTC.com was the top mining pool on both lists, and the largest production share was in China for both of the two prior lists. The second and third largest countries by cryptocurrency produced value are the US and Hong Kong. We note again, these are pools, so what we are tracking are the host locations. The annual economic value produced by the top pools increased from about $6 billion to about $8 billion between lists one and two.

The Third CryptoSuper list, released in conjunction with SC19

The CryptoSuper500 tracks decentralized supercomputers that are used for cryptocurrency mining, an intensive application that has become a driver of technology development and investment decisions globally. The growth of the cryptocurrency market has put the spotlight on emerging decentralized applications, the new ways in which they are funded, and the software stack on which they are built. Cryptocurrency technologies include blockchain, consensus algorithms, digital wallets, and utility and security tokens.

There are now over 4000 cryptocurrencies. Most are worth relatively little, and only 13 have market caps over $1 billion. Market cap is the number of coins or tokens outstanding times the price. In an extreme illustration of the Pareto principle, two-thirds of the market cap of all cryptocurrencies combined is with Bitcoin, the premier crypto.

There are different ways of creating new cryptos, different consensus algorithms or methods of solving the Byzantine generals' problem of preventing fraudulent transactions, e.g. double spending, a form of counterfeiting. The two most robust consensus algorithms from the security and value perspective are Proof of Work and Proof of Stake. But only Proof of Work is a computationally intensive process that leads to supercomputing levels of resources being assigned.

We consider here only the most valuable Proof of Work coins, starting with the ten most valuable by total market cap; these ten are summarized in Table 1. Of these ten, eight turn out to be of significance when we compile our list of the top 50 top mining pools. Dash and Dogecoin do not make the cut.

Table 1: Top 10 Mined Coins

Coin	Market Cap $B	HW	Algorithm	Block time	Block reward	New coins/day	Hash rate	units
Bitcoin	148.3	ASIC	SHA256	10 min.	12.5	1800	98.01	Exa
Ethereum	18.94	ASIC	Ethash	15 sec.	2	11,520	182.1	Tera
Bitcoin Cash	4.069	ASIC	SHA256	10 min.	12.5	1800	2.95	Exa
LTC	3.47	ASIC	Scrypt	2.5 min.	12.5	7,200	188.0	Tera
Bitcoin SV	1.692	ASIC	SHA256	10 min.	12.5	1,800	1.48	Exa
Monero	0.969	GPU	CryptoNight	2 min.	4.87	3,506.4	327.6	Mega
Dash	0.631	ASIC	X11	2.6 min.	1.55	892.8	4.91	Peta
Ethereum Classic	0.517	ASIC	Ethash	15 sec.	4	23,040	9.80	Tera
Dogecoin	0.332	ASIC	Scrypt	1 min.	10,000	14,400,000	195.0	Tera
Zcash	0.28	ASIC	Equihash	2.5 min.	10	5,760	5.07	Giga

In Table 1 we show the coin, its market cap at the end of October 2019, the type of hardware used in mining (usually specialized ASICs, and in one case GPUs), the mining algorithm, the time to mine a block and the number of coins rewarded to the first computer to solve the cryptographic problem and commit the block to the blockchain. We also show the new coins per day, a recent average hash rate, and the units associated with the hash rate. Bitcoin Cash and Bitcoin SV are hard forks away from the core Bitcoin blockchain. Only Bitcoin, Bitcoin Cash, and Bitcoin SV have hashrates that enter the Exa domain.

The information for this third edition of the CryptoSuper 500 list was collated on Halloween Day, 2019, which is the 11th anniversary date of the publication of the Satoshi Nakamoto white paper.

A Hundred Exahashes

Hashes in crypto mining are the metric that parallels flops in the supercomputing world.

Crypto miners compete via Proof of Work consensus algorithms in order to win a block reward and commit a group of transactions to the blockchain. Cryptocurrency mining via Proof of Work continues to represent the most effective class of consensus algorithm to maximize security in a decentralized manner, and to allow coins to accrue significant value.

In our CryptoSuper 500 race, we only look at the top mined coins that use Proof of Work, since these are the *only supercomputer class workloads* in the cryptocurrency world. Other consensus algorithms are much less costly, but as the marketplace has consistently demonstrated, impart much less value and security to a cryptocurrency. This is a trade-off between store of value and utility attributes.

Crypto mining entered the Exascale era in 2016; three years ago, the global hash rate for bitcoin was already exceeding an ExaHash per second. As of this writing, Bitcoin's total computational power is nearing 100 Exahashes per second. Crypto hashes are very simple calculations, using SHA(256) in the case of Bitcoin hashing, with many repeated trials required until a winning result adhering to the pre-defined problem difficulty is achieved.

The problem difficulty is regularly adjusted by the consensus algorithm as the collective hashrate increases or decreases. Bitcoin has had 300 such adjustments to data, on an approximate two-week schedule (each 2016 blocks).

Table 2 shows the Bitcoin hashrate history at one-half block year intervals, starting from when Bitcoin was two block years of age. Each block year is 52,500 blocks of approximately 10 minutes' duration, and block years are running slightly shorter than regular calendar years, recently by about two weeks. We are now in the 12th block year since Bitcoin's blockchain launched in January 2009.

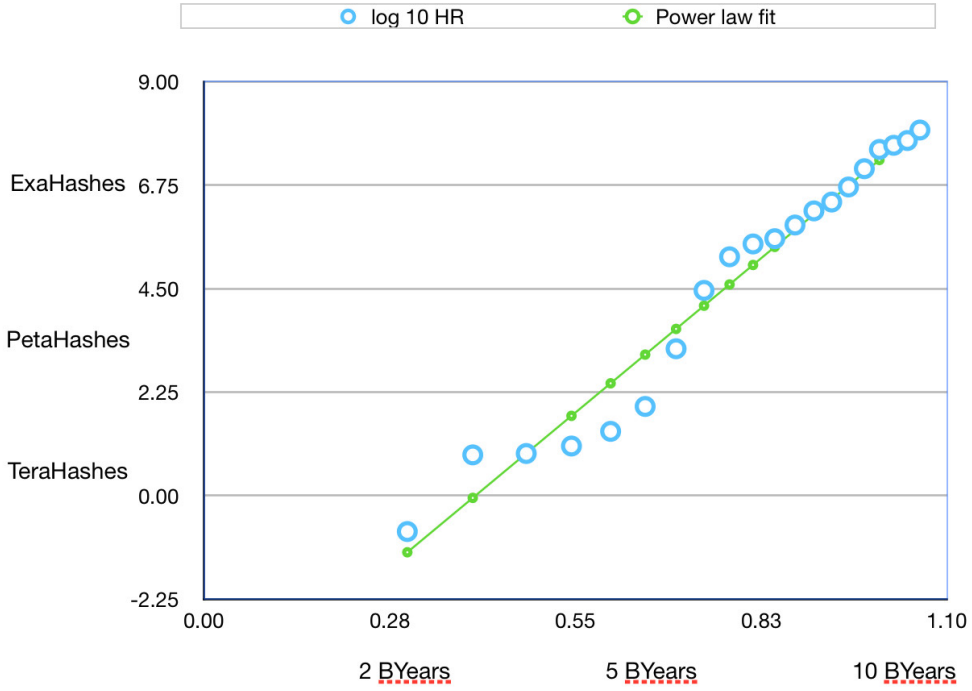
Table 2: Hashrate History of Bitcoin since year two

Block Height	Block reward	Block Years elapsed	Date	Hashrate (TeraH/s)	log 10 of Hashrate	log 10 of Block Year	Power law, 3-year interval
105,000	50	2	2011-01-28	0.166	-0.78	0.30	
131,250	50	2.5	2011-06-16	7.705	0.89	0.40	
157,500	50	3	2011-12-14	8.249	0.92	0.48	
183,750	50	3.5	2012-06-09	12	1.08	0.54	
210,000	25	4	2012-11-28	25	1.40	0.60	
236,250	25	4.5	2013-05-15	87	1.94	0.65	
262,500	25	5	2013-10-09	1564	3.19	0.70	7.82
288,750	25	5.5	2014-03-03	29,033	4.46	0.74	9.60
315,000	25	6	2014-08-11	156,187	5.19	0.78	14.83
341,250	25	6.5	2015-01-31	296,921	5.47	0.81	18.49
367,500	25	7	2015-07-29	386,597	5.59	0.85	19.37
393,750	25	7.5	2016-01-17	766,473	5.88	0.88	17.49
420,000	12.5	8	2016-07-09	1,554,081	6.19	0.90	13.15
446,250	12.5	8.5	2017-01-02	2,420,682	6.38	0.93	9.35
472,500	12.5	9	2017-06-23	5,145,068	6.71	0.95	8.46
498,750	12.5	9.5	2017-12-11	12,845,067	7.11	0.98	9.90
525,000	12.5	10	2018-05-29	33,710,000	7.53	1.00	12.10
551,250	12.5	10.5	2018-11-24	41,483,900	7.62	1.02	12.59
577,500	12.5	11	2019-05-24	52,657,000	7.72	1.04	12.26
603,750	12.5	11.5	2019-11-14	89,789,000	7.95	1.06	11.92
630,000	6.25	12	2020-05-xx				
Last 3 years	HR ratio	37.09		R^2	0.98	slope	12.20
	CAGR	233%				intercept	-4.90

In the table, the block height (number of blocks) is shown in the first column, then the block reward is shown in the following column. Note that it decreases by a factor of two each four block years; these are the key Halving events that drive inflation down toward zero. The calendar date is shown, then in the next column the total hashrate for all miners around the globe. Then we have the base 10 logarithm for the hashrate and the log of the block years elapsed. In the last column of the table one sees the 3-year prior interval slope for a log - log regression (power law relationship) between hashrate and block years.

The hashrate is up by over eight orders of magnitude in the past nine years. Hashrate has been growing extremely rapidly, roughly as the 12th power of elapsed block time! For a while in the 2014-15 period hashrate was growing with a power law > 15 as a rapid switch from GPUs to ASICs was underway. Now it has settled down somewhat to only being much, much faster than Moore's law.

Figure 1: Hashrate for Bitcoin for past nine and a half years
(log-log plot; abscissa is log Blockyears, green line is power law with exponent 12.20)



The price of Bitcoin, on the other hand, has been growing roughly as the 5th power of elapsed block time, driven by enhanced security and scarcity as Bitcoin's inflation rate drops continually. Hashrate follows price as miners are incentivized to increase their capital investment in terms of the number of systems devoted to mining and by obtaining the latest and greatest hardware. The result is that the hashrate is increasing at greater than the square of the Bitcoin price.

Doubling almost Twice a Year

In the last three calendar years, as indicated in Table 2, hashrate increased 37 times for Bitcoin, for a compound (calendar year) annual growth rate of 233%. This implies a doubling each seven months, or *over three times more rapidly than the Moore's law rate*.

Hashrate follows price, price reflects security (that depends on length of blockchain and hashrate as well) and scarcity (stock-to-flow, or inverse of the inflation rate) which is a simple function of blockchain length and more than doubles with each Halving at four block year intervals.

Mining inputs include capital equipment expense, facilities expense, personnel, electricity, cooling, as well as the expected price of bitcoin or other cryptocurrency, over the capital equipment life; various studies suggest a typical 50/50 capex/opex split.

Since the major equipment cycle is around two years, the miners must look out a couple of years ahead and guesstimate costs and future bitcoin price to justify new capital investment. If price drops they can shut down their least efficient (e.g. older) equipment and only mine with their newer equipment that has the best hashrate per kilowatt characteristics. There may also be seasonal effects, especially since a lot of the miners are located in

regions with cheap hydroelectric power that costs less when more water is flowing. If some miners shut in some equipment, the more efficient miners will increase their shares of bitcoin rewards, as the mining difficulty will decrease. Somebody gets the rewards.

Capex is sunk cost, so miners will continue to mine in the face of dropping prices as long as they can have positive cash flow after operating expenses (they may have to defer equipment upgrades, though, if cash is tight). They also can hedge their expected future production through forward sales with Bitcoin options or futures.

This rapidly growing global hashrate is a result of strong advances in the specialized rack-optimized crypto mining ASIC-based computer designs, in performance, packaging, and efficiency, and also in the optimization efforts of mining pools as they seek out the least costly locations for electrical power and cooling and optimize their facilities design. It is of course additionally a result of the long-term increase of Bitcoin price, some four orders of magnitude since early 2011.

Summary Tables

Here we present tables of the top mined coins, top mining countries, and top pool operators (including multiple coins mined by a single operator).

As shown in Table 3, the total annual economic value for the top 50 mining pools is $7.38 billion per year. This is down from the June 2019 list by a $1 billion or so. The Bitcoin price is up, but other coin prices have noticeably dropped since then. Ethereum is producing about half the economic value that it was in June. Of the top pools, 18 are mining Bitcoin, 9 are mining Ethereum, 7 are mining Bitcoin Cash, and 7 Litecoin. The other 4 major coins have between one and three entries each. *Bitcoin amounts to 84% of all of the economic value of the top 50 pools,* while Ethereum is another 10%. The remaining 6% is spread across the 6 other significant coins. The Pareto principle is very much in evidence here.

Table 3: Top eight coins that have mining pools in the Top 50

Coin	Top 50 Pools: M$ per year	Number entries in Top 50	Percent of Annual Economic Value
Bitcoin	6205.6	18	84.1
Ethereum	723.8	9	9.8
Bitcoin Cash	154.1	7	2.1
Litecoin	130.9	7	1.8
Zcash	58.9	3	0.8
Bitcoin SV	60.5	3	0.8
Monero	30.6	2	0.4
Ethereum Classic	12.4	1	0.2
Total	7376.7	50	100

Bitcoin has increased its dominance substantially just in the past six months. On our June 2019 list it was 66% of the economic value production (AEV, annual economic value). The #2 and #3 coins have fallen back in the past half-year with production only half of their prior AEV. Litecoin, now the #4 coin, has fallen to around 20% of its previous AEV.

Table 4: Top Host Countries

Host Country	Number of Top Pools	Percent of AEV	Annualized M$
China	20	43.8	3234
Global	5	14.7	1082
US, China	3	12.2	897
US	8	10	734
Hong Kong	5	8.2	607
Unknown	4	7.5	550
Other	5	3.7	272
Totals	50	100	7377

In Table 4 we show the top countries. China clearly dominates as before, with 44% of the annual economic value. When one considers that both the Global and the combined US plus China categories include Chinese mining as well, the Chinese share is roughly 55%, and adding in Hong Kong, about 63%. Including the US, China category assuming a 50/50 split, the US share is around 16%. Clearly the supposed crackdown on Chinese mining by their government is having limited impact. That crackdown is more about managing electricity usage, particularly seasonal issues around hydropower availability. Crypto mining has recently been removed from a Chinese government list of 'undesirable industries'.

Table 5 shows the Top 10 pool operators, combining multiple coins mined by a given operator. Some operators are mining four of the top coins. If the entry is in the top 50 for pools of a given coin, it is aggregated in this list. BTCdotcom is #1, F2Pool, a global pool, is #2, and Poolin which is located in both the US and China is #3. We see that five of the top 10 pool operators are in China. One is global, one is in Hong Kong, one is in the US, and one is located both in the US, and China.

Table 5: Top Pool Operators

Pool Operator	Host Country	Number of Top Pools	Annualized M$
BTC.com	China	3	1,129
F2Pool	Global	4	1,059
Poolin	US, China	3	897
AntPool	China	4	769
ViaBTC	Hong Kong	4	523
Unknown	n/a	1	469
Huobi.Pool	China	1	404
SlushPool	US	1	384
BTC.Top	China	2	374
SparkPool	China	1	234
Totals		24	6,241

Table 6a and 6b show sthe full list of the top 50 cryptocurrency mining pools around the world.

The AEV production for the top 50 mining pools has grown from about $5.4 billion to nearly $7.4 billion over the past year, up 37%. The #1 pool has grown its output by even more in percentage terms, from $0.7 billion to $1.1 billion, or around 62%.

Table 6a: Top 25 Mining Pools

Rank	Pool	Coin	Monthly M$	Annualized M$	Host Country
1	BTCdotcom	Bitcoin BTC	91.20	1,094.5	China
2	F2Pool	Bitcoin BTC	62.14	923.3	Global
3	Poolin	Bitcoin BTC	69.10	829.2	US, China
4	AntPool	Bitcoin BTC	60.61	727.3	China
5	ViaBTC	Bitcoin BTC	39.27	471.3	Hong Kong
6	Unknown	Bitcoin BTC	39.08	469.0	n/a
7	Huobi	Bitcoin BTC	33.69	404.3	China
8	Slush pool	Bitcoin BTC	32.01	384.1	US
9	BTCTop	Bitcoin BTC	29.48	353.8	China
10	Sparkpool	Ethereum ETH	19.49	233.9	China
11	Bitfury	Bitcoin BTC	17.21	206.5	Georgia, Iceland
12	Ethermine	Ethereum ETH	15.94	191.3	US
13	F2Pool	Ethereum ETH	8.32	99.8	China
14	NanoPool	Ethereum ETH	7.24	86.9	Global
15	BytePool	Bitcoin BTC	7.00	84.0	Hong Kong
16	1Thash	Bitcoin BTC	5.66	67.9	China
17	NovaBlock	Bitcoin BTC	5.32	63.8	US
18	Unknown	Bitcoin Cash BCH	4.54	54.5	n/a
19	Poolin	Litecoin LTC	3.09	37.0	US, China
20	MiningPoolHub	Ethereum ETH	3.04	36.5	Global
21	SpiderPool	Ethereum ETH	3.01	36.2	China
22	Way1 dot cn	Bitcoin BTC	2.94	35.3	China
23	Bitcoin dot com	Bitcoin BTC	2.68	32.1	US
24	Poolin	ZCash ZEC	2.53	30.4	US, China

All the long-term trends are strongly up for Bitcoin: hashrate, price and market cap, and the annual economic value of mining. The first year of the new decade will be very interesting, due to the Bitcoin intrinsic algorithmic Halving of supply emission, that is expected to occur in May, 2020.

Table 6b: Top 26-50 Mining Pools

Rank	Pool	Coin	Monthly M$	Annualized M$	Host Country
26	Bixin	Bitcoin BTC	2.14	25.7	China
27	BTCdotcom	Bitcoin Cash BCH	1.82	21.9	China
28	F2Pool	Litecoin LTC	1.74	20.9	Global
29	BTCTop	Bitcoin Cash BCH	1.67	20.1	China
30	Coingeek	Bitcoin SV	1.67	20.0	Canada
31	Litecoinpool	Litecoin LTC	1.54	18.5	US, EU
32	SupportXMR	Monero XMR	1.53	18.3	US
33	Bitclub	Bitcoin BTC	1.41	17.0	US
34	Okpool	Bitcoin BTC	1.38	16.5	China
35	qq4qnu	Bitcoin Cash BCH	1.35	16.2	China
36	Bitcoin dot com	Bitcoin Cash BCH	1.27	15.3	US
37	F2Pool	ZCash ZEC	1.23	14.8	Global
38	Ltcbtctop	Litecoin LTC	1.22	14.6	China
39	12VASaej	Bitcoin SV	1.21	14.5	n/a
40	0xd224..	Ethereum ETH	1.20	14.3	Germany
41	AntPool	Bitcoin Cash BCH	1.18	14.1	China
42	ViaBTC	Litecoin LTC	1.16	14.0	Hong Kong
43	AntPool	ZCash ZEC	1.15	13.8	China
44	AntPool	Litecoin LTC	1.14	13.7	China
45	PandaPool	Ethereum ETH	1.05	12.6	China
46	0xaa5c..	Ethereum ETH	1.03	12.4	n/a
47	Ethermine	Ethereum Classic ETC	1.03	12.4	US
48	MineXMR	Monero XMR	1.02	12.3	France
49	BTCdotcom	Litecoin LTC	1.02	12.2	China
50	ViaBTC	Bitcoin Cash BCH	1.00	12.0	Hong Kong

Quantum Blockchain?

A note on quantum supremacy. The threat comes from the future ability of quantum computers to crack ECDSA or other encoding schemes via Shor's algorithm or similar algorithms. The first vulnerability will be the wallets that store private keys to cryptocurrency. Shor's algorithm would allow a sufficiently powerful quantum computer to derive your private key from the public key that is recorded in the blockchain entries with your transactions, and one would need to migrate cryptocurrency to a quantum safe wallet. The blockchain itself will be threatened only at a later date.

How far off is this threat to keys? Estimates vary widely, it could be one decade or three, based on a range of models that have been examined. The community will need to come to a consensus on a quantum safe approach, and users will need to migrate to quantum-safe wallets. There are currently a number of efforts underway; the article linked above discusses XMSS, which has been recognized by NIST as post-quantum secure. Perhaps in the future we will all have portable cold atom quantum crypto wallets.

References, Data Sources

Cryptocurrency topics: orionx.net/blog

CryptoSuper 500 Second Edition, Shahin Khan, http://orionx.net/2019/06/cryptosuper500-2nd-edition/

Top Cryptocurrency Supercomputers June 2019, slide presentation, Stephen Perrenod
https://www.slideshare.net/perrenod/top-cryptosupers-201906v1-149547256

Overall statistics: coinmarketcap.com, coinwarz.com, cryptoslate.com

BTC: btc.com

ETH: btc.com, etherscan.io

BCH: btc.com, cash.coin.dance

Other coins: miningpoolstats.stream

"Quantum Supremacy and the case for Quantum Security Today in the Blockchain" Jack Matier, 2019 September, Medium, https://medium.com/the-quantum-resistant-ledger/quantum-supremacy-and-the-case-for-quantum-security-today-in-blockchain-390fe55daab5

Please visit OrionX.net/research for additional information and related reports.